UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY
TRENTON DIVISION

LEWIS CHEWNING, DAVID HEALEY, and BELLE ROSENBLOOM, Individually, and on Behalf of All Others Similarly Situated,	)	
Plaintiffs,	)	Case No. 3:23-cv-01227
v.	)	**JURY TRIAL DEMANDED**
CENTRASTATE HEALTHCARE SYSTEM, INC.	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiffs Lewis Chewning, David Healey, and Belle Rosenbloom ("Plaintiffs"), through their undersigned counsel, bring this action against CentraState Healthcare System Inc. ("CentraState" or "Defendant") pursuant to the investigation of their attorneys, personal knowledge as to themselves and their own acts and otherwise upon information and belief, and allege as follows:

INTRODUCTION

1. CentraState Healthcare System, Inc. is a hospital system with associated facilities, including an ambulatory campus, a charitable foundation, and three senior living centers.[1]

2. On or about December 29, 2022, CentraState experienced a hack and exfiltration of patient data, which it publicly reported on or about February 8, 2023 (the "Data Breach").

3. CentraState reported that this sensitive personal information ("SPI") included at least names, addresses, dates of birth, Social Security numbers, health insurance information,

[1] *See* https://www.centrastate.com/who-we-are/, last accessed February 24, 2023.

medical record numbers, and patient account numbers. CentraState further reported that for some individuals, this information also included information related to care received at CentraState, such as date(s) of service, physician names and departments, treatment plans, diagnoses, visit notes, and prescription information.[2]

4. Plaintiffs and Class members now face a present and imminent lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

5. The information stolen in cyber-attacks allows the modern thief to assume victims' identities when carrying out criminal acts such as:

- Filing fraudulent tax returns;
- Using the victim's credit history;
- Making financial transactions on behalf of victims, including opening credit accounts in victims' names;
- Impersonating victims via mail and/or email;
- Impersonating victims in cyber forums and social networks;
- Stealing benefits that belong to victims; and
- Committing illegal acts which, in turn, incriminate victims.

6. Plaintiffs' and Class members' SPI was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the SPI of Plaintiffs and Class members.

7. As of this writing, there exist many class members who have no idea their SPI has been compromised, and that they are at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

8. Plaintiffs bring this action on behalf of all persons whose SPI was compromised as

---

[2] *See* https://www.hipaajournal.com/hacking-and-data-theft-incident-reported-by-centrastate-healthcare-system/, last accessed February 24, 2023.

a result of Defendant's failure to: (i) adequately protect consumers' SPI, (ii) adequately warn its current and former customers and potential customers of its inadequate information security practices, and (iii) effectively monitor its platforms for security vulnerabilities and incidents (the "Class"). Defendant's conduct amounts to negligence and violates state statutes.

9. Plaintiffs and similarly situated individuals have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished inherent value of SPI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their SPI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) deprivation of rights they possess under common law and state statutes; and (v) the continued and certainly an increased risk to their SPI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the SPI.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

11. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is located within this District.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant resides within this judicial district and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

PARTIES

13. Plaintiff Lewis Chewning is a natural person residing in Monmouth County, New Jersey. Plaintiff Chewning's original Data Breach notification letter was sent to an address at which he no longer lives. However, on or about February 22, 2023, he was informed via a call to the number set up by Defendant that he had been a victim of the Data Breach and a new letter would be forthcoming to his current address.

14. Plaintiff David Healey is a natural person residing in Mercer County, New Jersey. On or about February 22, 2023, Plaintiff Healey was informed via a letter from Defendant that he had been a victim of the Data Breach.

15. Plaintiff Belle Rosenbloom is a natural person residing in Monmouth County, New Jersey. On or about February 22, 2023, Plaintiff Rosenbloom was informed via a letter from Defendant that she had been a victim of the Data Breach.

16. Defendant CentraState Healthcare System, Inc. is a not-for-profit New Jersey corporation with its principal place of business in Freehold, New Jersey.

FACTUAL ALLEGATIONS

17. Defendant is a hospital system with associated facilities located in Monmouth County, New Jersey.

18. Defendant sees at least tens, if not hundreds of thousands of patients a year at its facilities.

19. In the ordinary course of doing business with Defendant, patients provide Defendant or Defendant's client practices with SPI such as:

a. Contact and account information, such as name, usernames, passwords, address, telephone number, email address, and household members;

b. Authentication and security information such as government identification, Social Security number, security codes, and signature;

c. Demographic information, such as age, gender, and date of birth;

d. Payment information, such as credit card, debit card, and/or bank account number; and

e. Medical history as self-reported by patients, or medical history as transmitted from other healthcare providers;

20. On or about February 8, 2023, Defendant issued letters to affected patients that it had "detected unusual activity" on its computer systems and that an "unauthorized person obtained a copy of an archived database that contained patient information."

21. While Defendant states that it became aware of the Data Breach on December 29, 2022, it took more than a month for Defendant to begin to notify patients of the breach. At the time of this writing, CentraState has still not issued any public statements about the Data Breach and makes no mention of it on its website.

22. There exist many patients who do not reside at the address(es) CentraState has on file for them that have no idea that the Data Breach even occurred.

23. As a result, Plaintiffs' and class members' SPI was in the hands of hackers for an as-yet unknown amount of time before Defendant began notifying them of the Data Breach. Defendant has given no indication of when the Data Breach actually occurred – only when it first discovered the Data Breach.

24. Defendant has been vague on its response to the Data Breach, stating merely that, "[W]e are committed to the security of our systems."

25. As of this writing, Defendant has offered no detailed information on the steps it has taken or specific efforts made to reasonably ensure that such a breach cannot or will not occur again.

26. This response is entirely inadequate to Plaintiffs and class members who now potentially face several years of heightened risk from the theft of their SPI and who may have already incurred substantial out-of-pocket costs in responding to the Data Breach.

27. Defendant maintains a HIPAA Policy on its web page (which has not been updated in nearly a decade), noting various categories under which it may disclose treatment, payment, and healthcare information.[3] It lists several bases under which it may release protected health information without consent. However, releasing that information to hackers is not a disclosed category.

28. Defendant had obligations created by contract, industry standards, common law, state statute, and representations made to Plaintiffs and Class members, to keep their SPI confidential and to protect it from unauthorized access and disclosure.

29. Plaintiffs and Class members provided their SPI to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

30. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the industry preceding the date of the breach.

31. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a

[3] https://www.centrastate.com/hipaa-privacy-practices/, last accessed March 1, 2023.

warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

32. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[4] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[5]

33. The SPI of Plaintiffs and members of the Classes was taken by hackers to engage in identity theft and or to sell it to other criminals who will purchase the SPI for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

34. Defendant knew, or reasonably should have known, of the importance of safeguarding the SPI of Plaintiff and members of the Class, including Social Security numbers, dates of birth, and other sensitive information, as well as of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and members of the Class as a result of a breach.

35. Plaintiffs and members of the Class now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will

---

[4] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf, last accessed March 1, 2023.

[5] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

continue to incur such damages in addition to any fraudulent use of their SPI.

36. The injuries to Plaintiffs and members of the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the SPI of Plaintiff and members of the Class.

37. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

38. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

39. The FTC further recommends that companies not maintain SPI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

40. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take

to meet their data security obligations.

41. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer SPI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

42. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

43. Best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

44. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

45. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

46. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

47. The SPI of individuals remains of high value to criminals, as evidenced by the

prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[6]

48. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[7]

49. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

50. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited

---

[6] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs, last accessed March 1, 2023.

[7] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), https://www.ssa.gov/pubs/EN-05-10064.pdf, last accessed March 1, 2023.

into the new Social Security number."[8]

51. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[9]

52. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential SPI to mimic the identity of the user. The personal data of Plaintiff and members of the Class stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiff and the Class. Stolen personal data of Plaintiff and members of the Classes represents essentially one-stop shopping for identity thieves.

53. The FTC has released its updated publication on protecting SPI for businesses, which includes instructions on protecting SPI, properly disposing of SPI, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

54. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional

---

[8] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015),http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft, last accessed March 1, 2023.

[9] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), http://www.ssa.gov/pubs/EN-05-10064.pdf, last accessed March 1, 2023.

Requesters:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[10]

55. Companies recognize that SPI is a valuable asset. Indeed, SPI is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other SPI on a number of Internet websites. The stolen personal data of Plaintiff and members of the Class has a high value on both legitimate and black markets.

56. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

57. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Defendant's former and current customers whose Social Security numbers have been compromised now face a real, present, imminent and substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

58. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — Social Security number, driver license number or government-issued identification number,

[10] *See* https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29, last accessed March 1, 2023.

name, and date of birth.

59. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[11]

60. This is even more true for minors, whose Social Security Numbers are particularly valuable. As one site noted, "The organization added that there is extreme credit value in Social Security numbers that have never been used for financial purposes. It's relatively simple to add a false name, age or address to a Social Security number. After that happens, there is a window for thieves to open illicit credit cards or even sign up for government benefits."[12]

61. Among other forms of fraud, identity thieves may obtain driver licenses, government benefits, medical services, and housing or even give false information to police. An individual may not know that his or her driver license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

FACTS SPECIFIC TO PLAINTIFFS

62. On February 22, 2023, Plaintiff Chewning was informed, via a call to Defendant's hotline, that he was the recipient of a Data Breach notification letter which was sent to an address at which he no longer resides.

63. Plaintiff was a patient of Defendant in or around 2014, at which time he provided

---

[11] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed May 23, 2022)

[12] https://www.identityguard.com/news/kids-targeted-identity-theft (last accessed April 30, 2022)

his SPI to Defendant.

64. Had Plaintiff Chewning known that his SPI would not have been adequately protected by Defendant, he would not have used Defendant's services or he would have insisted that they not be stored in Defendant's system.

65. Since approximately December 30, 2022, Plaintiff Chewning has received numerous calls and text from various scammers purporting to offer various medical and medically-related services. This activity indicates that his information has been placed into the hands of hackers and has already been sold throughout the dark web.

66. Additionally, Plaintiff is aware of no other source from which the theft of his SPI could have come. He regularly takes steps to safeguard his own SPI in his own control.

67. On or about February 22, 2023, Plaintiff Healey was notified via a letter from Defendant that he had been the victim of the Data Breach.

68. Plaintiff was a patient of Defendant in or about December 2018, at which time he provided his SPI to Defendant.

69. Had Plaintiff Healey known that his SPI would not have been adequately protected by Defendant, he would not have used Defendant's services or he would have insisted that they not be stored in Defendant's system.

70. On or about February 28, 2023, Plaintiff Healey was informed that an account was attempted to be opened in his name at Bank of America.

71. Additionally, within the last six months, Plaintiff Healey has received numerous calls and text from various scammers purporting to offer various medical and medically-related services. This activity indicates that his information has been placed into the hands of hackers and has already been sold throughout the dark web.

72. Additionally, Plaintiff is aware of no other source from which the theft of his SPI could have come. He regularly takes steps to safeguard his own SPI in his own control.

73. On or about February 22, 2023, Plaintiff Rosenbloom was notified via a letter from Defendant that she had been the victim of the Data Breach.

74. Plaintiff has been a patient of Defendant since 1996, and has at various times provided her SPI to Defendant.

75. Had Plaintiff Rosenbloom known that her SPI would not have been adequately protected by Defendant, she would not have used Defendant's services or she would have insisted that they not be stored in Defendant's system.

76. Additionally, Plaintiff Rosenbloom is aware of no other source from which the theft of her SPI could have come. She regularly takes steps to safeguard her own SPI in his own control.

CLASS ACTION ALLEGATIONS

77. Plaintiffs bring this nationwide class action pursuant to Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following classes:

> All natural persons residing in the United States whose SPI was compromised in the Data Breach announced by Defendants on or about February 8, 2023 (the "Nationwide Class").

78. The New Jersey Subclass is defined as follows:

> All natural persons residing in New Jersey whose SPI was compromised in the Data Breach announced by Defendants on or about February 8, 2023 (the "New Jersey Subclass").

79. The New Jersey Subclass, together with the Nationwide Class, are collectively referred to herein as the "Classes" or the "Class."

80. Excluded from the Class are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to

hear any aspect of this litigation and their immediate family members.

81. Plaintiffs reserve the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

82. **Numerosity**: The Classes are so numerous that joinder of all members is impracticable. Defendant has, as of this writing, indicated that the total number of Class Members is in excess of two million. The Classes are readily identifiable within Defendant's records.

83. **Commonality**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual members of the Classes. These include:

a. When Defendant actually learned of the Data Breach and whether its response was adequate;

b. Whether Defendant owed a duty to the Classes to exercise due care in collecting, storing, safeguarding and/or obtaining their SPI;

c. Whether Defendant breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the SPI of Plaintiff and members of the Classes;

e. Whether Defendant acted negligently in connection with the monitoring and/or protection of SPI belonging to Plaintiff and members of the Classes;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep the SPI of Plaintiff and members of the Classes secure and to prevent loss or misuse of that SPI;

g. Whether Defendant has adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendant caused Plaintiff's and members of the Classes damage;

i. Whether Defendant violated the law by failing to promptly notify Plaintiff and members of the Classes that their SPI had been compromised;

j. Whether Plaintiff and the other members of the Classes are entitled to credit monitoring and other monetary relief;

k. Whether Defendant violated the New Jersey Consumer Fraud Act.

84. **Typicality**: Plaintiffs' claims are typical of those of the other members of the Classes because all had their SPI compromised as a result of the Data Breach due to Defendant's misfeasance.

85. **Adequacy**: Plaintiffs will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiff's counsel are competent and experienced in litigating privacy-related class actions.

86. **Superiority and Manageability**: Under rule 23(b)(3) of the Federal Rules of Civil Procedure, a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable. Individual damages for any individual member of the Classes are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

87. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Nationwide Class as a whole and as the New Jersey Subclass as a whole.

88. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and members of the Classes to exercise due care in collecting, storing, using, and safeguarding their SPI;

b. Whether Defendant breached a legal duty to Plaintiffs and the members of the Classes to exercise due care in collecting, storing, using, and safeguarding their SPI;

c. Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether members of the Classes are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

FIRST CLAIM FOR RELIEF
Negligence
(By Plaintiffs Individually and on Behalf of the Nationwide Class)

89. Plaintiffs hereby re-allege and incorporate by reference all of the allegations in paragraphs 1 to 90.

90. Defendant routinely handles SPI that is required of their patients, such as Plaintiffs.

91. By collecting and storing the SPI of its patients, Defendant owed a duty of care to the individuals whose SPI it collected to use reasonable means to secure and safeguard that SPI.

92. As a medical services provider, Defendant is aware of that duty of care to the SPI of its clients' patients.

93. Additionally, as a covered entity, Defendant has a duty under HIPAA privacy laws to protect the confidentiality of patient healthcare information, including the kind stolen as part of the Data Breach.

94. Defendant has full knowledge of the sensitivity of the SPI and the types of harm that Plaintiffs and Class Members could and would suffer if the SPI were wrongfully disclosed.

95. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of their current and former patients' SPI, and that of their beneficiaries and dependents, involved an unreasonable risk of harm to Plaintiffs and Class

Members, even if the harm occurred through the criminal acts of a third party.

96. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiffs' and Class Members' information in Defendant's possession was adequately secured and protected.

97. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and Class Members' SPI.

98. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

99. Plaintiffs and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of should have known of the inherent risks in collecting and storing the SPI of Plaintiffs and the Class, the critical importance of providing adequate security of that SPI, and the necessity for encrypting SPI stored on Defendant's systems.

100. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiffs' and Class Members' SPI, including basic encryption techniques freely available to Defendant.

101. Plaintiffs and the Class Members had no ability to protect their SPI that was in, and possibly remains in, Defendant's possession.

102. Defendant was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

103. Defendant had and continues to have a duty to adequately disclose that the SPI of Plaintiffs and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their SPI by third parties.

104. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the SPI of Plaintiffs and Class Members.

105. Defendant has admitted that the SPI of Plaintiffs and Class Members was purposely exfiltrated and disclosed to unauthorized third persons as a result of the Data Breach.

106. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the SPI of Plaintiffs and Class Members during the time the SPI was within Defendant's possession or control.

107. Defendant improperly and inadequately safeguarded the SPI of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

108. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect its current and former patients' SPI in the face of increased risk of theft.

109. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its current and former patients' SPI.

110. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and Class Members the existence and scope of the Data Breach.

111. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the SPI of Plaintiffs and Class Members would not have been compromised.

112. There is a close causal connection between Defendant's failure to implement security measures to protect the SPI of Plaintiffs and Class Members and the harm suffered or risk of imminent harm suffered by Plaintiffs and the Class. Plaintiffs' and Class Members' SPI was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such SPI by adopting, implementing, and maintaining appropriate security measures.

113. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their SPI is used; (iii) the compromise, publication, and/or theft of their SPI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their SPI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their SPI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the SPI of its patients and former patients in its possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the SPI compromised as

a result of the Data Breach for the remainder of Plaintiffs' and Class Members' lives.

114. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their SPI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the SPI in its continued possession.

SECOND CLAIM FOR RELIEF
Invasion of Privacy
(By Plaintiffs Individually and on Behalf of the Nationwide Class)

115. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 90.

116. Plaintiffs and the Class had a legitimate expectation of privacy to their SPI and were entitled to the protection of this information against disclosure to unauthorized third parties.

117. Defendant owed a duty to Plaintiffs and the Class to keep their SPI confidential.

118. Defendant failed to protect and released to unknown and unauthorized third parties the non-redacted and non-encrypted SPI of Plaintiffs and the Class.

119. Defendant allowed unauthorized and unknown third parties access to and examination of the SPI of Plaintiffs and the Class by way of Defendant's failure to protect the SPI.

120. The unauthorized release to, custody of, and examination by unauthorized third parties of the SPI of Plaintiffs and the Class is highly offensive to a reasonable person.

121. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and the Class disclosed their SPI to Defendant as part of Plaintiffs' and the Class' relationships with Defendant, but privately and with the intention that the SPI would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

122. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiffs' and the Class' interest in solitude or seclusion, either as to their persons or as to

their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

123. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

124. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and the Class.

125. As a proximate result of the above acts and omissions of Defendant, the SPI of Plaintiffs and the Class was disclosed to third parties without authorization, causing Plaintiffs and the Class to suffer damages.

126. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class in that the SPI maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

THIRD CLAIM FOR RELIEF
(Breach of Confidence)
(By Plaintiffs Individually and On Behalf of the Nationwide Class)

127. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 90.

128. At all times during Plaintiffs' and the Class' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and the Class' SPI that Plaintiffs and the Class provided to Defendant.

129. As alleged herein and above, Defendant's relationship with Plaintiff and the Class was governed by terms and expectations that Plaintiffs' and the Class' SPI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

130. Plaintiffs and the Class provided their SPI to Defendant with the explicit and implicit understanding that Defendant would protect and not permit the SPI to be disseminated to any unauthorized third parties.

131. Plaintiffs and the Class also provided their SPI to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect that SPI from unauthorized disclosure.

132. Defendant voluntarily received in confidence the SPI of Plaintiffs and the Class with the understanding that their SPI would not be disclosed or disseminated to the public or any unauthorized third parties.

133. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, the SPI of Plaintiffs and the Class was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs and the Class' confidence, and without their express permission.

134. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and the Class have suffered damages.

135. But for Defendant's disclosure of Plaintiffs' and the Class' SPI in violation of the parties' understanding of confidence, their SPI would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiffs' and the Class' SPI as well as the resulting damages.

136. The injury and harm Plaintiffs and the Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and the Class' PII and PHI. Defendant knew or should have known its methods of accepting and securing Plaintiffs' and the Class' SPI was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiffs' and the Class' SPI.

137. As a direct and proximate result of Defendant's breach of its confidence with Plaintiffs and the Class, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to decide how their SPI is used; (iii) the compromise and/or theft of their SPI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their SPI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover

from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their SPI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the SPI of Plaintiffs and the Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of their SPI as a result of the Data Breach for the remainder of Plaintiffs' and the Class Members' lives.

138. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

FOURTH CLAIM FOR RELIEF
Violation of the New Jersey Consumer Fraud Act,
N.J.S.A. § 56:8-1, *et seq*.
(By Plaintiffs Individually and on Behalf of the New Jersey Subclass)

139. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 90.

140. Defendant has violated N.J.S.A. § 56:8-1*, et seq*., by engaging in unconscionable, deceptive or fraudulent business acts and practices and omissions regarding the same as defined in N.J.S.A. § 56:8-2 with respect to the services provided to the Class.

141. Defendant engaged in unconscionable acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting the SPI of Plaintiffs and the Class with knowledge that the information would not be adequately protected; and by storing the SPI of Plaintiffs and the Class in an unsecure environment in violation of HIPAA and the rules and regulations promulgated thereunder, including 42 U.S.C. § 1301, *et seq*., 45 C.F.R. §§ 164.400-414, and 45 C.F.R. § 164.306, *et seq*. (as alleged *supra*.); and in violation of the Federal Trade Commission Act, 15 U.S.C. § 45 and 17 C.F.R. § 248.201, which require Defendant to employ reasonable methods of safeguarding the PII and PHI of Plaintiff and the Class.

142. Further, Defendant failed to inform Plaintiffs and the New Jersey Subclass that it had not undertaken sufficient measures to ensure the security of their SPI.

143. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiffs and the Class were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of Plaintiffs' and the Class' legally protected interest in the confidentiality and privacy of their SPI, nominal damages, and additional losses as described above.

144. Defendant knew or should have known that its data security practices were inadequate to safeguard the SPI of Plaintiffs and the Class and that the risk of a data breach or theft was highly likely, especially given its inability to adhere to basic encryption standards and data disposal methodologies. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Class.

145. Plaintiffs and the Class seek relief under N.J.S.A. § 56:8-2.12 and §56-8.19 including, but not limited to, restitution to Plaintiffs and the Class of money or property that Defendant may have acquired by means of Defendant's unconscionable business practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendant's unconscionable business practices, treble damages, declaratory relief, attorneys' fees and costs and injunctive or other equitable relief.

FIFTH CLAIM FOR RELIEF
Unjust Enrichment, in the Alternative
(By Plaintiffs Individually and on Behalf of the Nationwide Class)

146. Plaintiffs hereby re-allege and incorporate by reference all of the allegations in paragraphs 1 to 90.

147. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of storing their SPI with Defendant in such a way that saved expense and labor for Defendant.

148. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. Defendant also benefited from the receipt of Plaintiffs' and Class Members' SPI, as this was used by Defendant to facilitate its core functions.

149. The benefits given by Plaintiffs and Class Members to Defendant were to be used by Defendant, in part, to pay for or recoup the administrative costs of reasonable data privacy and security practices and procedures.

150. As a result of Defendant's conduct, Plaintiffs and Class Members suffered actual damages in an amount to be determined at trial.

151. Under principles of equity and good conscience, Defendant should not be permitted to retain a benefit belonging to Plaintiffs and Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and Class Members granted to Defendant or were otherwise mandated by federal, state, and local laws and industry standards.

152. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds or benefits it received as a result of the conduct alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request judgment against the Defendant and the following:

A. For an Order certifying the Class as defined herein, and appointing Plaintiffs and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and

the Class Members' SPI;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiffs and Class Members' personal identifying information;

iv. prohibiting Defendant from maintaining Plaintiffs' and Class Members' personal identifying information on a cloud-based database (if, in fact, it does so);

v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendant to engage independent third-party security auditors and

internal personnel to run automated security monitoring;

vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems

for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For pre- and postjudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY DEMAND

Plaintiffs hereby demand a trial by jury on all issues so triable.

DATED: March 2, 2023

Respectfully Submitted,

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP

/s/ Mark C. Rifkin
Mark C. Rifkin
270 Madison Ave.
New York, New York 10016
Tel: (212) 545-4600
Fax: (212) 686-0114
rifkin@whafh.com

Carl V. Malmstrom
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
111 W. Jackson Blvd., Suite 1700
Chicago, Illinois 60604
Tel: (312) 984-0000
Fax: (212) 686-0114
malmstrom@whafh.com

Counsel for Plaintiffs and the Putative Class